GOVERNMENT OF INDIA
COMMUNICATIONS AND INFORMATION TECHNOLOGY
LOK SABHA

UNSTARRED QUESTION NO:1816
ANSWERED ON:09.12.2015
Cyber Espoinage
Adityanath Shri Yogi;Muddahanumegowda Shri S.P.;Natterjee Shri J. Jayasingh Thiyagaraj;Patil Shri Bheemrao Baswanthrao;Ranjan (Pappu Yadav) Shri Rajesh;Reddy Shri Ch. Malla;Sawant Shri Arvind Ganpat

Will the Minister of COMMUNICATIONS AND INFORMATION TECHNOLOGY be pleased to state:

(a) whether there have been instances of hacking of the Governmental websites/breach of sensitive information from critical sectors of Government in the country during the last three years and the current year and if so, the details thereof;

(b) whether there is a plan to develop a pan-India secure network/network-based services to provide foolproof infrastructure for telecom and internet communication of the Government, if so, the details thereof;

(c) whether adequate software security system has been installed to check hacking in view of the sensitive nature of information available on the Government websites and if so, the details thereof;

(d) whether any special cell has been constituted to find out the websites hacked by people outside the country, and to restore it and if so, the details thereof; and

(e) the details of measures/activities taken by the National Critical Information Infrastructure Protection Centre (NCIIPC) to safeguard the country's critical sectors from cyber-threats and cyber-attacks?

Answer

(a): As per the information reported to and tracked by Indian Computer Emergency Response Team (CERT-In), a total number of 371, 189, 155 & 128 Government websites were hacked during the year 2012, 2013, 2014 and 2015 (upto October) respectively. The Government websites host information for public dissemination. No sensitive information is hosted on Government websites. As per the guidelines of the Government, the Computer systems with sensitive information are isolated from Internet.

(b): As per information from Department of Telecommunications, a Secure and Dedicated Communication Network (SDCN) designed for provision of 5000 secured phones has been planned for intra-Government Communication initially at Delhi to be scaled up to 20000 users for entire country. The System is currently under installation and Testing.

(c): In order to protect the websites of Government departments a layered security approach in the form of practices, procedures and technologies is put in place. National Informatics Centre (NIC) that hosts the Government websites has deployed state-of-the-art security solutions including firewall, intrusion prevention systems and anti-virus solution.

CERT-In issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis. CERT-In has published guidelines for securing the websites, which are available on its website (www.cert-in.org.in). CERT-In also conducts regular training programmes to make the system administrators aware about secure hosting of the websites.

In addition, all Central Government Ministries / Departments and State / Union Territory Governments have been advised to conduct security auditing of entire Information Technology infrastructure. All the new government websites and applications are to be audited with respect to cyber security prior to their hosting. The auditing of the websites and applications is to be conducted on a regular basis even after hosting.

(d): Indian Computer Emergency Response Team (CERT-In) regularly tracks the hacking of websites and alerts the website owners concerned to restore the hacked websites and taking actions to secure the websites to prevent recurrence. The National Informatics Centre (NIC) is operating a security monitoring centre for detecting and responding to security incidents. Restoration of the affected website is done after taking necessary remedial measures.

(e): National Critical Information Infrastructure Protection Centre (NCIIPC) has been operationalised as per the provisions of Section 70A of the Information Technology Act 2000, for protection of Critical Information Infrastructure in the country. NCIIPC has taken up the following measures/activities for protection of critical sectors:-

i) Assisting critical sector organizations in undertaking vulnerability / threat / risk assessment of their cyber security infrastructure
ii) Issuing advisories on software/hardware vulnerabilities and alerts on cyber attacks regularly to Chief Information Security Officers of Critical Information Infrastructure

iii) Analysis of the policy documents, audit reports, compliance reports and cyber incident reports
iv) Assistance in identification of critical information infrastructure elements
v) Assistance in the development of policies, plans and adoption of standards
vi) Conducting trainings and awareness programs on critical information infrastructure
vii) Interfacing with organizations at state level for assessing the cyber security status of infrastructure

****